DATE(S) ISSUED:
10/13/2010

SUBJECT:
Vulnerability in Windows Media Player Could Allow Remote Code Execution (MS10-082)

OVERVIEW:
A vulnerability has been identified in Microsoft Windows Media Player. Windows Media Player is a digital media player and media library application that is used for playing audio, video, and viewing images. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

        Windows XP
        Windows Server 2003
        Windows Vista
        Windows Server 2008
        Windows 7

RISK:
Government:
        Large and medium government entities: **High**
        Small government entities: **High**

Businesses:
        Large and medium business entities: **High**
        Small business entities: **High**

Home users: **High**

DESCRIPTION:
A remote code execution vulnerability has been discovered in the way Microsoft Windows Media Player un-assigns objects during a reload operation in a Web browser. This vulnerability may be exploited if a user visits a specially crafted web page. It should be noted that the vulnerability will not be exploited automatically as the user will need to first click through a series of pop-up dialog boxes for the exploit to be successful.

Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:
- Apply the appropriate patch provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:
Microsoft:
http://www.microsoft.com/technet/security/bulletin/MS10-082.mspx

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-2745